IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098- WMW-JFD

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION FOR PARTIAL RECONSIDERATION OF THE COURT'S AUGUST 1, 2023 ORDER

INTRODUCTION

Plaintiffs Smartmatic USA Corp., Smartmatic International Holding B.V. and SGO Corporation Limited ("Smartmatic") brought a defamation lawsuit against Defendants Michael J. Lindell and My Pillow, Inc. for statements Lindell made about voting machines used in the 2020 Presidential Election, including Smartmatic's. Smartmatic asserts that Lindell's statements caused some undisclosed portion of its purported $2 billion decline in business valuation. (ECF No. 125, Compl. ¶ 365.)

Among the requests for production directed to Smartmatic, Defendants sought the source code for any Smartmatic product and an exemplar of a ballot marking device ("BMD") used in the 2020 Presidential Election. This discovery is squarely relevant to the claims and defenses in this case. Smartmatic refused and Defendants moved to compel. On

August 1, 2023, the Court issued an order denying Defendants' motion, primarily because Defendants could this discovery by issuing a subpoena to Los Angeles County, the only county which used Smartmatic equipment in the 2020 Presidential Election. (ECF No. 160 at 19.)

However, while Defendants' motion to compel was under advisement, counsel for Los Angeles County notified defense counsel that the county deleted the source code in 2022. In addition, despite multiple phone calls and emails, counsel for the county has failed to inform Defendants whether Los Angeles County even has an exemplar BMD in its possession, much less produce one. Consequently, on August 7, 2023, Defendants sought permission to bring a motion for partial reconsideration based on this new information. (ECF No. 165.) On August 18, 2023, the Court granted Defendants' request. (ECF No. 169.)

The inspection of Smartmatic's source code and BMD are critical to the claims and defenses in this case. There can be no dispute that this discovery is relevant and nonprivileged. Any confidentiality concerns can be addressed by an attorneys' eyes only designation and the protective order, which includes a specific method – *drafted by Smartmatic* – to provide for additional measures to protect this discovery.

To date, Smartmatic and Los Angeles County have delayed and stonewalled in an apparent attempt to run out the clock on discovery. Smartmatic told Defendants to obtain the discovery from third-party, Los Angeles County, which, despite this lawsuit and the receipt of Defendants' litigation hold letter, deleted the source code, and has refused to provide the BMD or even confirm whether the county has possession of the device.

Defendants have no means to acquire this discovery other than from Smartmatic, the party which brought this lawsuit in the first place. The Court should order Smartmatic to comply with its discovery obligations and produce this information without further delay.

BACKGROUND

On January 18, 2022, Smartmatic sued Defendants for defamation seeking $2 billion in damages for statements Lindell made about voting machines used in the 2020 Presidential Election, including Smartmatic's. (ECF No. 1.) Smartmatic alleged in part, that Lindell's statements about Smartmatic were not and could not be true because Smartmatic's election technology, hardware and software were only used in Los Angeles County. (*Id*. ¶ 134.) Defendants moved to dismiss the complaint, and that motion was denied on September 19, 2022. (ECF No. 52.)

A couple of weeks before that order was issued, Defendants' counsel sent Los Angeles County a "Notice of Litigation and Document Preservation Notice" requesting that the county preserve, among other things, all evidence regarding its "election voting system and the data created by or related to the election voting system." (Declaration of Abraham S. Kaplan ("Kaplan Decl.") Ex. A.)

On November 4, 2022, Defendants served Smartmatic with discovery requests seeking in part, "[a]n exemplar of each Smartmatic Product used by any county, precinct, election site, or polling location in the State of California to administer the 2020 Presidential Election[,]" and the "source code for any for any Smartmatic Product, Hardware, Software, or systems used in the 2020 Presidential Election in any county,

precinct, election site, or polling location in the State of California." (ECF No. 76-1 at 11, Requests for Prod. Nos. 1 and 8.)

Smartmatic refused to produce any discovery responsive to these requests, and after a failed attempt to meet and confer, on February 1, 2023, Defendants moved to compel. (ECF No. 75, Defs.' Mem. at 4.) In response, Smartmatic claimed that it did not have possession, custody or control of the source code because it turned it over to Los Angeles County, where it was put in escrow, before the 2020 election. (Doc. 89 at 12-15.) Although Smartmatic had access, but not current possession of this discovery, Smartmatic asserted that Defendants should instead subpoena *third-party* Los Angeles County for Smartmatic's source code and BMD. (*Id*. at 21.)

On February 7, 2023, Defendants issued a subpoena to the Los Angeles County Registrar-Recorder/County Clerk. (Kaplan Dec. Ex. B.) The subpoena, which was served on February 14, 2023, sought, in pertinent part, a copy of the source code and an inspection of an exemplar device used by Los Angeles County in the 2020 Presidential Election. (*Id*.) On February 28, 2023, Los Angeles County served its objections to the subpoena. (*Id*. Ex. C.)

Defendants' counsel called and emailed counsel for the county several times between approximately late April and early May 2023, requesting a meet and confer. (*Id*. ¶ 5; Ex. D.) Counsel for Defendants met and conferred with Los Angeles County's counsel at least twice regarding Defendants' requests. (*Id*. ¶¶ 5, 10, 13; Ex. D.) On June 14, 2023, counsel for Los Angeles County informed Defendants' counsel that the county no longer possessed the escrowed version of the source code. (*Id*. ¶ 10.) Notwithstanding this

litigation and the county's receipt of a litigation hold letter from Defendants' counsel in September 2022, counsel for Los Angeles County stated that the escrowed source code was deleted "sometime in 2022." (*Id*.; Ex. A.)

Since August 1, 2023, Defendants have continued their efforts to obtain discovery responsive to the subpoena. (*Id*. ¶¶ 10-14.) Although the county had already deleted the source code, Defendants still hoped to inspect an exemplar BMD. Between August 1 and August 7, 2023, defense counsel emailed counsel numerous times asking that the parties expeditiously resolve the issues because of the impending discovery deadline of August 25. (*Id*. ¶ 11.) The county's counsel did not respond. (*Id*.) However, on August 7, 2023, a *different attorney* representing Los Angeles County called Defendants' counsel. Defense counsel proposed narrowing the requests and again inquired about what responsive information remains in the county's possession. (*Id*. ¶ 12.) Although this attorney stated that the first attorney with whom defense counsel had been conferring with for months would respond in short order, both attorneys for Los Angeles County "went dark," and Defendants have heard nothing further from the county. (*Id*. ¶¶ 12-15.) Therefore, almost seven months after the subpoena was served, counsel for Los Angeles County has failed to answer that question, or produce any responsive discovery. (*Id*. ¶¶ 13-15; Ex. D.)

In its Order dated August 1, 2023, the Court ordered the following with respect to the BMD exemplar and source code:

> Smartmatic has credibly asserted that it does not have the materials Defendants seek. Given the sensitivity of source code and the numerous *alternative means, including a Rule 45 subpoena*, *available to Defendants for obtaining information about the Smartmatic products used on Election Day 2020*, the Court finds that the burden of producing the source code

> outweighs its potential relevance and thus will not require that Smartmatic provide it.

(ECF No. 160 at 19.) (Emphasis added.)

One of the Court's main reasons for denying the motion to compel was Defendants' alternative means of obtaining the information from Los Angeles County. (ECF No. 160 at 19.) That alternative means no longer exists. The only available copies of the source code reside with Smartmatic's independent testing authority, which Smartmatic has confirmed it can and will produce upon order from this Court. (Doc. 89 at 17) (citing Plaintiff's contract with Los Angeles County, Declaration of Michael Bloom ¶ 3, Ex. 1 § 7.8.3, ECF No. 91-1) ("Disclosures which are required by law, such as a court order, . . . are allowable."); (ECF. No. 108, Hr'g Tr. 26:1–28:14, 78:24–79:23.) Moreover, Los Angeles County has failed to confirm whether it has an exemplar BMD in its possession, much less produced such a device for inspection. (Kaplan Decl. ¶¶ 10-15; Ex. D.)

ARGUMENT

The Court should Amend its Order dated August 1, 2023, and compel Smartmatic to produce its source code and an exemplar BMD.

A. Smartmatic has access to the discovery, which is relevant to the claims and defenses in this case.

Federal Rule of Civil Procedure 26(b)(1) provides that a party "may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). This rule is to be "liberally construed." *NOW, Inc. St. Paul Chapter etc. v. Minn. Mining & Mfg. Co*., 73 F.R.D. 467, 472 (D. Minn. 1977) (citing *Hickman v. Taylor*, 329 U.S. 495, 507 (1947)).

Smartmatic sued Lindell for an incredible $2 billion in damages for various statements and implications including the following: Smartmatic rigged the 2020 Presidential Election; Smartmatic's products were connected to the internet; and Smartmatic's products were compromised or hacked by foreign countries. (*Id.* ¶¶ . (ECF No. 119, Compl. ¶¶ 365, 158, 166 and 173.)

To prevail on its defamation claim, Smartmatic must prove that Lindell's statements regarding Smartmatic's products are false. *Rouse v. Dunkley & Bennett, P.A.*, 520 N.W.2d 406, 410 (Minn. 1994). As a public figure, Smartmatic also must prove that the statements were made with "actual malice." *New York Times Co. v. Sullivan*, 376 U.S. 254, 279–80 (1964); (ECF NO. 52 at 6) (holding that Smartmatic is a public figure).

Conversely, Defendants may prevail in this case by showing that Lindell's statements are substantially true or, whether true or not, that they are not "inherently improbable." *See Armstrong v. Thompson*, 80 A.3d 177, 183-84 (D.C. App. 2013) (substantial truth defense to defamation claims); *St. Amant v. Thompson*, 390 U.S. 727, 732 (1968) (defamation plaintiff subject to "actual malice" standard must show the defamatory statements were either believed by the defendant to be false or were not made in good faith, which may be supported by evidence that the statements were "inherently improbable"). By claiming Lindell's statements were defamatory, Smartmatic placed at issue the truth and/or probability of the statements that Smartmatic machines were hacked or otherwise vulnerable to attack during the 2020 election.

The truth or the inherent probability of Lindell's statements about Smartmatic's equipment would be supported by evidence that the source code contained computer code

which could lead to the miscounting of votes. The truth or inherent probability of these statements would also be supported by evidence that the source code can be connected to the internet and that it's vulnerable to unauthorized access or programming changes.[1] To gather evidence probative of this issue, Defendants' counsel and experts must be allowed to inspect the source code. Such an inspection would provide information about whether Smartmatic's products could be used to attack the election or manipulate election results, whether Smartmatic's technology was susceptible to hacking by China or other foreign countries, and whether Smartmatic's products were capable of being connected to the internet.

Simply put, the inherent probability of Lindell's statements about Smartmatic equipment and the 2020 Presidential Election are of central importance to the defense that the statements at issue were made in good faith, *i.e.*, lacked "actual malice" under applicable First Amendment law.

There is not and cannot be any serious dispute that Smartmatic's software and hardware – the very subject of this lawsuit – is relevant to the claims and defenses in this case. While Smartmatic's responses to Requests Nos. 8 and 10 included a boilerplate lack of relevance objection, Smartmatic properly abandoned that argument in its opposition to Defendants' First Motion to Compel and implicitly conceded the relevance of this

[1] For example, BMDs employ a Quick Response Code ("QR Code") which make the device vulnerable to attack. *E.g., Curling v. Raffensperger*, Case No. 1:17-cv-02989-AT, (N.D. Ga.), ECF No. 168114 at 14) ("Attackers could cause the BMDs to print QR codes that differ from voters' selections while leaving the human-readable text of the ballot unchanged." This could lead to "a change to the tabulation of those individual votes affected and potentially to the election results.")

discovery. (ECF No. 76-1 at 21, 25; ECF No. 89, Pls.' Mem. at 11-29.) Indeed, Smartmatic plainly anticipated the production of such discovery when it included the following provision in the parties' stipulated protective order entered on November 3, 2022 ("Protective Order"):

> To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

(ECF No. 70, Protective Order ¶ 2; *see also* ECF No. 108, Hr'g Tr. at 82:9-17) (Plaintiffs' statement that if Defendants' motion were granted, "inspection and not wholesale production is the appropriate mechanism to do so, given the significant security concerns and the highly confidentiality [sic] nature of this material. *And I think that's something the parties could potentially work out a protocol for inspection*[.]") (Emphasis added.)

Smartmatic initiated this lawsuit. Smartmatic has access to its source code and BMD device, which are plainly relevant to the claims and defenses in this case. This discovery is not protected by any privilege, and there is no other sound basis to prohibit its disclosure. Smartmatic should be compelled expeditiously to produce its technology for inspection in accordance with the law, and a specific inspection protocol contemplated by Smartmatic in the Protective Order.

B. A specific protective order providing for an AEO designation and the selection of a neutral third-party laboratory to conduct the forensic imaging of the source code and BMD, would provide sufficient protection to alleviate any confidentiality concerns.

Smartmatic argues that it should not be compelled to disclose the relevant source code or BMD exemplar because of confidentiality concerns. In so doing, Smartmatic

pointedly ignores the substance of the Protective Order, which includes *a specific method – drafted by Smartmatic – to protect the source code*. (ECF No. 70 ¶ 2; *see also id.* ¶¶ 3-5; ¶¶ 8-11.) Rather than asserting that the Protective Order lacks sufficient provisions to protect the information, Smartmatic effectively argues that the Protective Order is rendered impotent because Lindell made public statements about obtaining discovery in order to reveal his '"truth' to the world." (ECF No. 89, Pls.' Mem. at 1; *id*. at 22-24.) This is a red herring. Smartmatic may designate sensitive information, including the source code and BMD device as "Attorneys' Eyes Only" pursuant to the Protective Order. (ECF No. 70, Protective Order ¶ 2.)

Further, the existing protective order contemplates a process to protect the *source code*: "the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected." (*Id*.) An additional protective order could also address the BMD exemplar. In *U.S. Dominion, Inc., et al., v. My Pillow, Inc., et al.*, a similar case in the United States District Court for the District of Columbia, Defendants sought the plaintiff's software and voting machine equipment used in the 2020 Presidential Election. Judge Carl Nichols entered a protective order which provided that the parties agree on a neutral third-party laboratory to conduct the forensic imaging of the equipment and software. (*U.S. Dominion, Inc., et al., v. My Pillow, Inc., et al.*, Civil Action No. 1:21-cv-445 (CJN), ECF No. 159.) The same process could be used in this case. Defendants' counsel has already suggested SLI Compliance for the forensic imaging work, which is the same company which examined and certified Smartmatic's machines prior to their use in Los Angeles County. (Kaplan Decl. ¶ 5.)

Plaintiffs' claim that "nondisclosure is the safest way to protect the confidentiality" of the information is not a serious argument. Nondisclosure is certainly the safest way to protect *any* information. But the rules expressly contemplate that sensitive information can be produced in a specific manner so that it may remain confidential and provides penalties if court orders are violated. *See* Fed. R. Civ. P. 26(c)(1)(G) (allowing for a protective order to direct how trade secrets or other confidential research, development, or commercial information is disclosed); Fed. R. Civ. P. 37(b)(2) (setting forth available penalties for non-compliance with discovery orders).

Even where discovery involves the production of commercially sensitive information from one competitor to another – which is not true here – such information must still be produced. *See, e.g., Northbrook Digital, LLC v. Vendio Servs*., 625 F. Supp. 2d 728, 744-45 (D. Minn. 2008) (allowing discovery of confidential technical information but restricting the individuals who could review the information).

An AEO designation and detailed protective order setting forth a specific protocol related to the source code and BMD exemplar would prevent the parade of horribles Smartmatic describes. (ECF No. 89, Pls.' Mem. at 21-24.) With such protections in place, Lindell would have no access to the software or BMD device. Lindell would not be able to see it, let alone share it with the public. (ECF No. 89, Pls' Mem. at 22-24.) Defendants' counsel and experts would faithfully abide by an AEO designation and further protective order. Should any violation occur (it will not), the "Court will retain jurisdiction . . . to the extent necessary to enforce any obligations . . . or to impose sanctions for any violation thereof." (ECF No. 70 ¶ 29.) Concerns regarding the sensitivity of the technology ring

hollow considering the protections provided by an AEO designation and a carefully tailored protective order, particularly when weighed against the obvious relevance of this information in a bet-the-company lawsuit.

C. Defendants cannot properly prepare a defense without Smartmatic's source code and BMD exemplar.

Smartmatic should not be allowed to use the confidential nature of the information to refuse to produce the technology it created, which is squarely relevant to the claims it brought, as well as the defenses in this case. But just as Smartmatic has failed to produce its damages calculations so late in the game, Smartmatic is using its purported confidentiality concerns to further hide the ball by preventing Defendants' from inspecting the very software and technology which Smartmatic asserts, for example, is air -gapped and therefore, somehow invulnerable to hacking. (ECF No. 125 ¶143.)

An expert report analyzing Georgia's BMD devices manufactured by Dominion Voting Systems casts doubt on Smartmatic's claims about the safety of such air-gapped technology. Smartmatic's BMD devices, which are the same or similar to those used in Georgia, are vulnerable to attack, regardless of the "self-contained" nature of the technology. As the expert explained in *Curling v. Raffensperger*:

> Nation-state actors . . . have developed a variety of techniques for infiltrating non-Internet connected systems, including by compromising hardware and software supply chains . . . and by spreading malware on removable media that workers use to copy files in and out of protected environments.

(Case No. 1:17-cv-02989-AT, (N.D. Ga.), ECF No. 168114 at 12.) In this case, Smartmatic has restricted Defendants' ability to have their experts inspect Smartmatic software and equipment. Without such an expert inspection, Defendants will have no ability to disprove

Smartmatic's allegations to this effect, and thereby establish Defendants' lack of actual malice. Plainly, Defendants must be able to inspect Smartmatic's technology to prepare a defense. The Court should put an end to Smartmatic's gamesmanship and order it to produce the source code and exemplar BMD device after the parties have negotiated a more detailed protective order, just as Judge Nichols ordered in the Dominion case.

CONCLUSION

For the forgoing reasons, Defendants respectfully request that the Court grant their Motion for Partial Reconsideration of the Court's order dated August 1, 2023, and order Plaintiffs to make the source code and exemplar BMD available to Defendants for inspection pursuant to an appropriate protective order.

DATED: September 1, 2023

PARKER DANIELS KIBORT LLC

By */s/ Abraham S. Kaplan*
Andrew D. Parker (MN Bar No. 195042)
Joseph A. Pull (MN Bar No. 0386968)
Abraham S. Kaplan (#399507)
Nathaniel R. Greene (#390251)
888 Colwell Building
123 N. Third Street
Minneapolis, MN 55401
Telephone: (612) 355-4100
parker@parkerdk.com
pull@parkerdk.com
kaplan@parkerdk.com
greene@parkerdk.com

ATTORNEYS FOR DEFENDANTS